TESTIMONY OF

HOWARD R. "SKIP" ELLIOTT

VICE PRESIDENT — PUBLIC SAFETY AND ENVIRONMENT

CSX TRANSPORTATION, Inc.

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

HEARING ON TSA'S SURFACE INSPECTION PROGRAM

MAY 31, 2012

CSX TRANSPORTATION
500 WATER STREET
JACKSONVILLE, FLORIDA 32202
904-359-3100

ASSOCIATION OF AMERICAN RAILROADS
425 THIRD STREET SW
WASHINGTON, DC 20024
202-639-2100

On behalf of CSX Transportation, Inc. (CSX) and the Association of American Railroads (AAR), thank you for the opportunity to appear before you today to discuss freight rail security issues in general and the Transportation Security Administration's (TSA) rail inspection program in particular.

CSX operates a freight rail network spanning approximately 21,000 miles, with service to 23 eastern states, the District of Columbia and two Canadian provinces. We are part of a 140,000-mile U.S. freight rail network that serves nearly every industrial, wholesale, retail, agricultural, and mining-based sector of our economy. Whenever Americans grow something, eat something, mine something, make something, turn on a light, or get dressed, CSX or some other freight railroad is probably involved somewhere along the line.

Amtrak and several commuter railroads are members of the AAR and they work in concert with CSX and other freight railroads on security matters. Indeed, the rail industry has established a dedicated Freight and Passenger Coordinating Committee, for which security is a primary area of emphasis. However, my testimony today will focus on freight railroads. My understanding is that Amtrak will present its own testimony at this hearing.

Assuring the security of our rail network requires a multi-faceted, cooperative effort that taps the full range of capabilities in the private sector and at all levels of government — including, of course, at the TSA — and applies them to best effect to assure preparedness and to deter and respond to acts of terrorism. CSX and our nation's other railroads work continuously to meet this objective.

At the same time, railroads want rail security to continue to improve, and they are always willing to work cooperatively with members of this committee, others in Congress, the TSA, other agencies in the Department of Homeland Security, the Federal Railroad Administration, rail labor, and others to find practical, effective ways to make this happen.

The Rail Industry Security Plan

Last fall our nation observed the 10th anniversary of the tragic 9/11 attacks. In previous appearances before this and other committees, rail industry representatives have detailed the many actions the industry took in the aftermath of those attacks.[1] I won't repeat those particulars here, but it is well documented that the rail industry voluntarily developed and implemented a Terrorism Risk Analysis and Security Management Plan, a comprehensive, intelligence-driven, priority-based blueprint of actions designed to enhance railroad security. The plan was adopted by the rail industry in December 2001 and remains in effect today. And much has been done since the initial voluntary efforts by the rail industry following September 11, 2001.

This means that before there was a TSA, before there was a DHS, the railroads had developed and implemented a unified, risk-based approach to security based on terrorism alert levels and progressively increasing protective measures to elevate preparedness to counter and respond to threats.

The security plan is not simply something that has been put on a shelf to be taken down and dusted off occasionally. Rather, it is a robust and dynamic paradigm for rail operations that is evaluated and modified, as necessary, to ensure maximum continued effectiveness and includes network-wide risk assessments and asset specific countermeasures focused on people, process, and technology. A comprehensive review completed in 2009 evaluated the plan's guiding assumptions, risk methodology, and countermeasures, yielding an updated version that took effect in November of that year. Since then, as the nature of the terrorist threat has evolved, the plan has been reviewed to ensure its continuing effectiveness. As the federal government has adjusted its procedures — most recently on terrorism alerts with the adoption of the National Terrorism Advisory System — the rail industry has made sure that its plan's alert level process and accompanying protective measures align well with the new federal procedures.

Regular exercises, conducted both industry-wide and by the railroads individually, appraise the effectiveness of the industry's security plan. Lessons learned from these exercises and from actual security-related incidents help ensure that the plan continues to evolve to meet changing circumstances and needs.

[1] See, for example, the statement of Edward R. Hamberger of the AAR before the Committee on Homeland Security on March 6, 2007, and the statement of Thomas L. Farmer of the AAR before the Subcommittee on Transportation Security and Infrastructure Protection on July 12, 2011.

The most recent industry-wide exercise occurred on October 13, 2011. For that event, the industry invited direct participation by several federal entities — including the TSA, DHS, FBI, and the FRA — specifically to assure effective implementation of an efficient, understandable, and sustainable process for sharing intelligence on security threats and incidents by federal government agencies with the rail industry.

The Rail Security Working Committee

A standing industry committee, comprised of senior railroad executives, security officials, and police chiefs, coordinates the rail industry's overall security effort. Supported by AAR's security staff, this group — known as the Rail Security Working Committee — reflects the industry's ongoing commitment to working in a coordinated fashion, with participation by all the major railroads.

Through monthly consultations, the committee identifies issues of concern, develops appropriate responses to those issues, and works with public sector partners to implement solutions. The review, exercise, and continuous improvement of the industry security plan, outlined above, are a vital facet of the committee's functions. For example, the committee has developed and implemented an industry-wide emergency notification system to provide immediate awareness to railroads of the most significant security incidents affecting a freight or passenger train. The notification system has been successfully tested twice already this year.

The committee also participates in open and candid discussions with TSA's Freight Rail Branch on current programs and initiatives, future priorities, and prevailing security issues and concerns, including those discussed further below. This continuing dialogue, which is held under the auspices of the Freight Rail Branch's Intermodal Security Training and Exercise Program (I-STEP), sustains constructive relationships and effective communication between the railroads' security and law enforcement officials and their counterparts in the government.

Information Sharing

Useful intelligence and security information must be shared in a timely, effective, and consistent manner if rail security efforts are to succeed. In this regard, railroads helped build and maintain two key resources focused on security information needs.

The first — the Surface Transportation Information Sharing and Analysis Center (ST-ISAC) — was formed by the rail industry in 2002 at the request of the U.S. Department of

Transportation. Working in secure facilities, ST-ISAC operates 24 hours a day, 7 days a week at up to the top secret level to collect, analyze, and distribute security information from a wide range of government, academic, media sources.

With the high profile that cybersecurity concerns have garnered recently, it is important to note the vital role the ST-ISAC plays to help protect rail information technology systems and physical assets from attack. Each day, the ST-ISAC issues several advisories to the railroads addressing potential vulnerabilities in specific software or equipment and providing guidance on protective measures. These materials provide timely awareness of current or emerging threats and concerns and inform the sustained preparedness that is the essential foundation of the railroads' coordinated approach to cybersecurity.

The second resource is the Railway Alert Network (RAN). The RAN serves as the rail industry's intelligence and security information center. Each day, its staff reviews intelligence, including classified information, from a broad range of sources and provides railroads with notice of and security advisories on rail-related threats, incidents, and suspicious activity.

In addition, because security threats and incidents impacting railroads can emerge in other critical infrastructure sectors, the RAN works with a private sector coordination group and other DHS components to ensure that railroads have relevant information on homeland security concerns generally.

The RAN's products include a concise brief produced each day in concert with the American Public Transportation Association and the ST-ISAC called the Transit and Rail Intelligence Awareness Daily (TRIAD) as well as focused security awareness messages that address rail security implications of threats, incidents, disrupted plots, and intelligence analyses. Examples of the RAN's output have been provided to this subcommittee for your information and reference prior to this hearing. The RAN shares most of the materials it produces and disseminates with our federal partners and with appropriate local and state authorities.

Information sharing is a two-way street, though, and unfortunately, CSX and the rail industry have found that information sharing by various government agencies with the rail industry is plagued by persistent difficulties in timeliness, practical security relevance, and means of dissemination. Railroads provide a plethora of security-related information every day to various governmental entities, but this reporting yields comparatively very little in analyses of security value for the industry.

The reporting to the Transportation Security Operations Center (TSOC) is a case in point. By regulation, railroads report "significant security concerns" to TSOC. There does not seem to be any process in place for analysis of these reports, and those in other surface transportation modes, for trends or other indicators of concern. Nor do the criteria for this mandated reporting align with those applied by the rest of DHS, the FBI, and the Office of Director of National Intelligence in the cross-sector Nationwide Suspicious Activity Reporting Initiative. Common reporting parameters, which the Rail Security Working Committee has formally proposed, would facilitate the inter-agency analysis and cross-sector sharing that is essential to continuous situation awareness and sustained security preparedness.

Railroads are proud of their ability to react quickly and decisively in the face of credible intelligence impacting the rail network. However, the sluggishness and inconsistency with which we receive important intelligence information hinders our ability to respond to potential threats. Railroads will continue to work amicably and professionally with our public sector partners to resolve this problem. Demonstrative of this commitment, and worthy of commendation, is a new initiative by TSA's Office of Intelligence, announced at a joint I-STEP meeting held in Newark this past March. That office has adopted the rail industry's most significant intelligence requirement as a priority in its analyses, shifting focus to thorough review of past terrorist attacks, failed attempts, and disrupted plots that have targeted rail worldwide – passenger and freight – for lessons learned and inferences on likely future tactics in order to inform more effective and sustainable security measures and actions. TSA analysts will consult with rail industry security leads in the development of these products. We will work in concert to ensure their effective dissemination, integrating local and State law enforcement departments as a means of fostering informed partnerships for security enhancement. This coordinated effort flows directly from consultations in the joint I-STEP meetings sponsored by TSA's Freight Rail Branch – and puts into practical application Assistant Secretary John Pistole's commitment that TSA is an intelligence-focused agency.

Working With the TSA and TSA's Rail Security Inspectors

CSX believes that partnerships are key to effective security planning and enhancing public safety, and that this cooperation provides lasting benefits to our employees and to the communities we serve. I'm sure the other freight railroads agree with us on this point. I'm also sure that, like CSX, the other railroads are proud of the collaborative working relationship the industry has developed in recent years with the TSA, DHS and other government entities.

This collaborative relationship is manifest in a variety of ways. For example, TSA's Freight Rail Branch has initiated recurring coordination meetings with railroads. As demonstrated by the progress on the rail industry intelligence requirement, this forum fosters effective communication and problem-solving, and we commend the Freight Rail Branch for establishing them via the I-STEP process. The most recent coordination meeting took place in Newark, New Jersey, during March 7-8, 2012.

Railroads also work effectively with TSA on a variety of training-related issues. For example, the Transportation Technology Center, Inc. (TTCI), a wholly-owned subsidiary of the AAR in Pueblo, Colorado, is the world's finest rail research facility. Among many other things, TTCI trains thousands of emergency responders each year from all over the country. Taking advantage of TTCI's expertise, TSA has been using TTCI for employee training since 2006. In fact, more than 2,100 TSA participants have trained at TTCI to date, in such areas as "Railroads 101," hazmat transportation, motor carrier security and safety compliance, and basic explosives. In 2010, TSA opened its own dedicated facility at TTCI, though it continues to draw upon the expertise of TTCI personnel in railroad training and orientation programs. The industry values this effective partnership.

The cornerstone of CSX's public-private partnerships is sharing our highly-specialized secure Network Operations Workstation ("SecureNOW") with federal and state homeland security officials. The SecureNOW system is a proprietary, secure online computer tool used to monitor, identify and respond to rail-security and emergency issues throughout the CSX network. This system, developed by CSX, provides CSX employees and trained state homeland security and public agency officials with a tool to promptly identify the location and status of CSX trains and rail cars on our network. SecureNOW allows trained security and public agency officials in several states to independently track the location of CSX trains and the contents of the rail cars in those trains in a nearly real-time environment. Before, officials needed to telephone CSX to access this information.

CSX’s SecureNOW system and our approach to information sharing helps homeland security officials prepare for and - if needed - respond to emergency situations. Access to SecureNOW also provides state and federal officials with additional information about what is carried on our rails, and state officials can more efficiently allocate law enforcement resources, coordinate with CSX security officials, and integrate rail security into on-going law enforcement operations.

In fact, CSX has entered into partnerships with two federal entities - the TSA’s TSOC and the DOT’s Crisis Management Center. This allows trained federal homeland security officials to have nearly real time information regarding the location of CSX trains and the contents of the rail cars transported on our lines. In addition to these federal partnerships, CSX also has partnerships for access to SecureNOW with New York, New Jersey, Kentucky, Maryland, Indiana, Ohio, Georgia, Florida. These partnerships formalize and enhance CSX's ongoing commitment to these states and federal agencies to share information, resources and strategies in order to better protect the communities in which CSX operates.

There are many other examples of successful cooperative initiatives involving the TSA and railroads, and railroads appreciate the TSA for its role in ensuring these successes. That said, we respectfully suggest that there are also some areas where additional progress could and must be made.

For example, as members of this committee know, the TSA has fielded more than 400 “Surface Transportation Security Inspectors” (STSIs) whose duty is to “assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security against terrorist attack and other security threats and to assist the Secretary in enforcing applicable surface transportation security regulations and directives.”[2]

[2] 6 USC 1113

Freight railroads readily acknowledge that the rail inspection program is well intended. At the same time, though, CSX and the rail industry have several concerns regarding the surface transportation inspection program.

First, CSX is very troubled by the lack of consistency in STSIs' interpretation of, and action on, regulatory requirements, especially with respect to the transport of hazardous materials. Different TSA STSIs have interpreted specific provisions of the Rail Transportation Security Rule in different ways, and provided contradictory guidance regarding what actions are and are not acceptable in meeting the rule's requirements. Actions accepted as compliant by some TSA field offices have been labeled violations that produce official citations by others. Indeed, CSX and other railroads have found that TSA field offices, and STSIs often disagree on how to interpret the rule. CSX and other railroads have also seen disparities between the policies and guidelines issued by TSA's Freight Rail Branch and the actions of TSA inspectors in the field. Sometimes, STSIs are not even aware of policies that have been clearly expressed by the Freight Rail Branch to the railroads they're inspecting.

Second, it is unfortunate that STSIs' enforcement efforts seem to focus on issues that, frankly, are fairly trivial and do not represent meaningful homeland security breaches. For example, the Rail Transportation Security Rule requires that shippers, receivers, and carriers of hazardous materials implement "chain of custody" requirements for rail cars carrying certain highly hazardous materials. Among other things, the transfer of custody from a shipper to a railroad, from one railroad to another railroad, and from a railroad to a receiver must be documented, with the railroad identifying by name the individual with the interchanging railroad, the shipper, or the receiver who is present at the time of transfer of custody. CSX has received warnings for non-compliance with the chain of custody rule because the names of the individuals attending the transfer of custody were not spelled the same way as the names on the interchanging railroad's form, even if they were phonetically identical.

CSX respectfully suggests that variations in the spelling of the names of the individuals attending the transfer of custody do not present a meaningful security breach, especially since the STSIs frequently have witnessed the properly executed transfer of custody and because spelling variations are inevitable when information is verbally exchanged (as specifically allowed by TSA guidance on the issue). In fact, these warnings for misspelling have been brought forth by

STSIs who, at the same time, offer praise for the execution of a flawless person-to-person hand off of these chemicals, attesting to compliance with the intended security enhancement of the regulation.

This example is not isolated. Experience at other freight railroads is similar. The inspections focus overwhelmingly on paperwork, elevating administrative errors to the level of official letters of investigation sent to railroads expressly citing the prospect of a $10,000 fine. To be candid, this type of approach to regulatory enforcement impugns the integrity of the hardworking professionals who strive very hard every day at CSX and other railroads to perform vital transportation services safely, efficiently, and in often difficult conditions. More importantly, situations like this breed distrust and ill-feelings for no good reason. They certainly do not advance the cause of security enhancement. Furthermore, as the U.S. freight rail system continues to advance its use of technology and paperless processes, TSA's implementation of a regulation that adheres to the use of cumbersome manual procedures is inconsistent with modern-day security solutions. CSX respectfully suggests that TSA resources should be focused on technology solutions that can provide bona fide enhancements to freight rail and national security.

We believe that the lack of consistency and standardization in inspection priorities and activities noted above is related to the organizational hierarchy regarding the STSIs. Our understanding is that STSIs do not report to the TSA Freight Rail Branch or to a TSA headquarters official responsible for surface transportation. Rather, STSIs report to Federal Security Directors ("FSD") in the field who primarily focus on aviation security and lack the subject matter expertise on surface transportation regulations and policies. This arrangement promotes inconsistency of understanding, application, and enforcement of security regulations and policies. Although TSA appointed Regional Security Inspectors (RSIs) to be liaisons to the railroads on surface transportation issues, the RSIs are not in the chain of command of the STSIs in the field or the TSA Freight Rail Branch and therefore lack the authority to resolve these issues or the ability to provide meaningful subject matter guidance on freight rail security issues. The appointment letters sent to the railroads in April 2010 state the RSIs are the "technical specialist within OSO [Office of Security Operations] at the national level for compliance oversight activities" and serve as "points of contact for the Class I and Regional Railroads for matters of regulatory compliance," with the goal "to ensure consistent application of regulations both nationally and across a railroad's operating system." The railroads have advocated strongly in joint meetings held by TSA, at which officials of OSO have participated, for integration of the RSIs into the oversight role defined in their appointment letters. In practice, the RSIs have not ever actually played this role.

Finally, CSX is also concerned that STSIs directly engage rail employees in the field without communicating or coordinating with the designated Rail Security Coordinator ("RSC"). The Rail Transportation Security Rule requires railroads (and other covered entities) to designate one primary and at least one alternate Rail Security Coordinator (RSC) at the corporate level. At least one RSC must be available to TSA 24 hours a day, 7 days a week. The RSC serves as the "primary contact for intelligence information and security related activities and communications with TSA." Additionally, the RSC is to coordinate "security practices and procedures with appropriate law enforcement and emergency response agencies."

If STSIs identify issues in the field, they should be communicating with the headquarters-based RSC, since the STSIs lack the authority and means to address the issues with our employees in the field. As TSA explained in the preamble to the final rule, "the RSC must be in a position to understand security problems, raise issues with corporate leadership, and recognize when emergency response action is appropriate." Indeed, CSX headquarters personnel cannot take steps to address issues identified by TSA in the field if TSA does not communicate those issues to us. Our discussions with our counterparts at other railroads indicate this is not just an issue for CSX.

Visible Intermodal Prevention and Response Teams (VIPR)

The rail industry acknowledges the potential value of the VIPR program's random and unpredictable security measures for deterrence and disruption of terrorist planning and preparations. Indeed, some railroads have hosted deployments and derived substantial benefits from the visible security enhancement. We remain concerned, though, about inconsistency in the implementation of this program — both in management (conflicts and duplications between TSA field offices) and in execution of operations (continuing instances of inadequate notice to and coordination with railroads on operations).

In September 2011, the Rail Security Working Committee defined protocols to govern the conduct of VIPR operations with freight railroads. These protocols, which comport with the provisions of the authorizing legislation for the VIPR program, consist of the following key points:

- Prior notice to the Rail Security Coordinator (RSC) by TSA of all proposed VIPR deployments at least two weeks in advance, unless a credible threat or other emergency circumstances dictate otherwise.
- To assure consistency, efficiency, and timeliness, coordination with the RSC to be made by the TSA RSI for the participating freight railroad.
- Rail safety training and orientation for all participants in the operation.
- Joint development by TSA and the affected railroad(s) of the operations plan for each VIPR deployment or group of deployments.
- Integration of local law enforcement in the VIPR deployment(s) to foster informed partnerships and elevated preparedness for joint security enhancement actions.
- Clearly stated risk-based justifications for the deployments.
- Priority attention in joint planning and execution of VIPR deployments at or near the approaches to security control points identified in the rail network identified by TSA's Freight Rail Branch in assessments conducted with the railroads.

The freight railroads are applying these protocols. However, a formal agreement with TSA has proven elusive, apparently due to differences amongst the main offices within the agency involved in the VIPR program.

Conclusion

CSX and others in the rail industry recognize and sincerely appreciate the diligent efforts made by TSA, and the many other local, state, and federal personnel who work hard every day to help keep our rail network, and our nation in general, safe and secure. We share their goals. Safety and security are, and will remain, our top priority.

That said, we recognize that the freight rail industry and the national security environment in which we operate are continually changing and new challenges appearing. Effective security enhancement can only happen if all stakeholders are on the same page and if sufficient consideration is given to the real-world effects (including unintended consequences) possible approaches to security policy can have. Genuine, open communication between railroads and government security personnel can not only lead to practical solutions, but can also open the door to solutions that might not otherwise have been apparent.

CSX and other freight railroads look forward to continuing to engage in constructive, meaningful dialogue with member of this committee, TSA, DHS, and others to ensure that our nation's railroads remain the most productive, the most efficient, and the safest and most secure in the world.